

My REU Experience

Morgan Burcham
University of North Alabama
Louisiana State University, Center for
Computation & Technology

Mentor: Dr. David Koppelman



Research Problem

- Return-oriented programming (ROP) attacks
 - It's all about the attacker...
 - Reproduce pieces of the original (good guy's) code.
 - Creates a Turing complete set of gadgets.
 - Uses gadgets to write attack code.
 - Gets the code into memory.
 - Links the code with return instructions.
 - Defenses exist but at the cost of efficiency.

Goal of the Research

To find a more efficient (low-overhead) defense, of course!

The Proposed Defense

- Will monitor instruction execution.
 - If we go to a new page in memory which will create a Turing complete set, we will lock other pages so the Turing complete set will be nonexistent.
 - Otherwise, we are not dealing with a Turing complete set, and execution will continue as normal.
 - When a page is first unlocked, the entry instruction will be checked for credibility.

What I Did This Summer

- Got to learn about a particular problem (ROP attacks) in the world of cybersecurity.
- More experience programming in low-level languages.
 - MIPS
 - Some exposure to Intel 64.
- Machine encoding
- Disassembly
- Implementation of gadget classes

Future Plans

- Research at UNA in Spring 2015.
 - Would love to continue doing research in cybersecurity area.
- B.S. in Computer Science in Spring 2015.
- Plan to attend graduate school to get a Ph.D. in Computer Science.
 - Concentration in Computer Security
- Goal is to be a computer science professor.

Acknowledgments

- Dr. James Jerkins - University of North Alabama, Department of Computer Science
- Dr. Janet Jenkins – University of North Alabama, Department of Computer Science
- Dr. David Koppelman
- Louisiana State University, Center for Computation & Technology
- National Science Foundation

Questions?